

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No. .... 10/816,083  
Filing Date..... 3/31/2004  
Confirmation No. .... 9450  
Inventorship..... David Y. Jao  
Assignee ..... Microsoft Corporation  
Group Art Unit..... 2135  
Examiner ..... KIM Y. VU  
Attorney's Docket No. .... MS1-1956US  
Title: USE OF ISOGENIES FOR DESIGN OF CRYPTOSYSTEMS

**INFORMATION DISCLOSURE STATEMENT AND  
CERTIFICATION UNDER 37 CFR 1.97(e)**

The listed citations were cited in a Communication from a foreign patent office in a counterpart foreign application, and are being submitted in compliance with the duty of disclosure defined in 37 CFR §1.56. Copies of the citations and the Communication are attached. The Examiner is requested to make these citations of official record in this application.

I hereby certify that each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement.

Furthermore, each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart application and this communication was not received by any individual designated in §1.56(c) more than thirty days prior to the filing of the information disclosure statement.

Respectfully Submitted,

Date: 12-28-2005

By: Frank J. Bozzo  
Frank J. Bozzo  
Reg. No. 36756

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

# INFORMATION DISCLOSURE STATEMENT BY APPLICANT

*(Use as many sheets as necessary)*

**Complete if Known**

|                        |              |
|------------------------|--------------|
| Application Number     | 10/816,083   |
| Filing Date            | 3/31/2004    |
| First Named Inventor   | David Y. Jao |
| Art Unit               | 2135         |
| Examiner Name          | KIM Y. VU    |
| Attorney Docket Number | MS1- 1956US  |

|       |   |    |   |
|-------|---|----|---|
| Sheet | 1 | of | 2 |
|-------|---|----|---|

## U. S. PATENT DOCUMENTS

[illegible]

**FOREIGN PATENT DOCUMENTS**

| FOREIGN PATENT DOCUMENTS |           |   |                                |   |   |    |
|--------------------------|-----------|---|--------------------------------|---|---|----|
| Examiner Initials*       | Cite. No. | Foreign Patent Document                     | Publication Date<br>MM-DD-YYYY | Name of Patentee or Applicant of Cited Document | Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear | T* |
|                          |           | Country Code*~Number*~Kind Code* (if known) |                                |   |   |    |
|                          |           | EP 1 215 642 - A1                           | 6/19/2002                      | HITACHI LTD (JP)                                |   |    |
|                          |           | WO 00/14924                                 | 3/16/2000                      | CITIBANK NA (US)                                |   |    |
|                          |           | WO 99/30458                                 | 6/17/1999                      | SECURED INFORMATION                             |   |    |
|                          |           |   |                                |   |   |    |
|                          |           |   |                                |   |   |    |
|                          |           |   |                                |   |   |    |

|                       |                    |
|-----------------------|--------------------|
| Examiner<br>Signature | Date<br>Considered |
|-----------------------|--------------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language translation is attached.

This collection of information is required by 37 CFR 1.87 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

**If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

**INFORMATION DISCLOSURE  
STATEMENT BY APPLICANT**

(Use as many sheets as necessary)

**Complete if Known**

|                            |                        |              |
|----------------------------|------------------------|--------------|
| Sheet <b>2</b> of <b>2</b> | Application Number     | 10/816,083   |
|                            | Filing Date            | 3/31/2004    |
|                            | First Named Inventor   | David Y. Jao |
|                            | Art Unit               | 2135         |
|                            | Examiner Name          | KIM Y. VU    |
|                            | Attorney Docket Number | MS1- 1956US  |

**NON PATENT LITERATURE DOCUMENTS**

| Examiner<br>Initials* | Cite<br>No. <sup>1</sup> | Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published. | T <sup>2</sup> |
|-----------------------|--------------------------|---|----------------|
|                       |                          | T. BETH and F. SCHAEFER, "Non Supersingular Elliptic Curves for Public Key Cryptosystems," Advances in Cryptology-Eurocrypt '91, Lecture Notes in Computer Science, 547 (1991), Springer-Verlag, pgs. 316-327.  |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |
|                       |                          |   |                |

|                       |                    |
|-----------------------|--------------------|
| Examiner<br>Signature | Date<br>Considered |
|-----------------------|--------------------|

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.